In the Claims:

1. (original) A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) generating a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN.

2. (original) A method as recited in claim 1, wherein the SCN is transferred to the money source in an account number and the first entity identifier is transferred to the money source in a non-account data field.

3. (original) A method as recited in claim 1, wherein the first entity identifier is transferred to the money source as an account number and the SCN is transferred to the money source in a non-account data field.

4. (currently amended) A method as recited in claim 3, wherein the TIB ~~can be~~ is used for invoking one or more restrictions on use of the SCN.

5. (currently amended) A method as recited in claim 4, wherein the TIB is used by the money source to determine whether the SCN ~~should be~~ is a single-use SCN or a multiple-use SCN.

6. (original) A method as recited in claim 5, wherein the TIB is used by the money source to identify a physical device used to generate the SCN.

7. (original) A method as recited in claim 6, wherein the encrypted PIN Block is formed by using a Triple Data Encryption Standard algorithm ("TDES") to encrypt a PIN Block.

8. (original) A device as recited in claim 7, wherein the PIN Block is generated from a PIN associated with the first entity, a Sequence Insertion Number ("SIN") and a starting value known to both the first entity and to the money source.

9. (original) A method as recited in claim 8, wherein the SIN is a combination of a first set of seed values and a random value generated by a Pseudo Random Number Generator ("PRNG") that was initialized with the first set of seed values.

10. (original) A method as recited in claim 9, wherein the first set of seed values consists of three seed values.

11. (original) A method as recited in claim 10, wherein the first set of seed values is associated with a Counter value

12. (original) A method as recited in claim 11, wherein the Counter Block is associated with the Counter value.

13. (original) A method as recited in claim 12, wherein the money source validates the SCN by duplicating a PIN Block encryption process used to create the encrypted PIN and by then comparing the result to the encrypted PIN Block received with the first transaction.

14. (original) A method as recited in claim 13, wherein the SCN is a nine digit number, the SCN Type is a one digit number, the Counter Block is a four digit number, and the encrypted PIN Block is a four digit number.

15. (original) A method as recited in claim 14, wherein the encrypted PIN Block is created by dividing an 8-byte Sequence Insertion Number ("SIN") into four 2-byte integers, adding the PIN and a pre-assigned constant 4-digit value to each of the four 2-byte integers, concatenating the results to form an 8-byte input block which the TDES encrypts into an 8-byte output block, dividing the 8-byte output block into four 2-byte integers x1, x2, x3 and x4 and then using integers x1-x4 in Formula 1 to produce the 4-digit encrypted PIN Block with a value P, wherein Formula 1 is P=(Ax1 + Bx2 + Cx3 + Dx4) mod 10000, each of the values A, B, C and D being pre-assigned odd integers.

16. (original) A method as recited in claim 15, wherein each of the three seed values and the random value is a 2-byte integer.

17. (original) A method as recited in claim 16, wherein an electronic card generates the SCN.

18. (original) A method as recited in claim 16, wherein a PIN is entered into an input device to generate the SCN.

19. (original) A method as recited in claim 18, wherein the SCN and first entity identifier are transferred to the second entity in a form.

20. (original) A method as recited in claim 19, wherein the SCN is transmitted through an Address Verification System Billing Address.

21. (currently amended) A method as recited in claim 20, wherein a unique SCN is assigned to each first entity which is valid only for mail order, telephone order, or internet transactions, and which ~~can be~~ is used for multiple transactions with multiple merchants.

22. (original) A method as recited in claim 21, wherein the second entity uses the SCN to authenticate the first entity.

23. (currently amended) A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) using an electronic card to generate a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN;

wherein the TIB ~~can be~~ is used for invoking one or more restrictions on use of the SCN; and

wherein the SCN is transferred to the money source in an account number and the first entity identifier is transferred to the money source in a non-account data field.

24. (currently amended) A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) using an electronic card to generate a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN;

wherein the TIB ~~can be~~ is used for invoking one or more restrictions on use of the SCN; and

wherein the SCN is readable by a magnetic card reader.

25. (currently amended) A method as recited in claim 24, wherein the SCN is readable from either a Track 1 or a Track 2 of the ~~magnetic~~ electronic card.

26. (currently amended) A method for providing one or more secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) using an electronic card to generate a Secure Card Number ("SCN") for the first entity, wherein the SCN is comprised of:

(a) a Transaction Information Block ("TIB");

(b) a Counter Block; and

(c) an encrypted Personal Identification Number ("PIN") Block;

(2) transferring the SCN and a first entity identifier to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN;

wherein the TIB ~~can be~~ is used for invoking one or more restrictions on use of the SCN; and

wherein the TIB is used by the money source to determine which of a plurality of account numbers associated with the first entity should be used for the first transaction.

27. (new) A method for providing a secure transaction between a first entity and a second entity comprising:

(1) generating a Secure Card Number ("SCN") for the first entity, wherein the SCN comprises a dynamic digital signature;

(2) transferring the SCN in a non-account data field and a first entity identifier in an account data field to a second entity in a first transaction;

(3) transferring the SCN and the first entity identifier from the second entity to a money source; and

(4) verifying that the first transaction is valid with the money source by use of the first entity identifier and the SCN.

28. (new) A method as recited in claim 27, wherein the first entity identifier is transferred to the money source as an account number.

29. (new) A method as recited in claim 27, wherein the dynamic digital signature is formed by using a Triple Data Encryption Standard algorithm ("TDES").

30. (new) A method as recited in claim 27, wherein the dynamic digital signature comprises an encrypted PIN.

31. (new) A method as recited in claim 27, wherein the dynamic digital signature is, at least in part, encrypted, and wherein the money source validates the SCN by duplicating a dynamic digital signature encryption process and by then

comparing the result to the dynamic digital signature received with the first transaction.

32. (new) A method as recited in claim 27, wherein an electronic card generates the SCN.

33. (new) A method as recited in claim 27, wherein a PIN is entered into an input device as a part of the generation of the SCN.

34. (new) A method as recited in claim 27, wherein a unique SCN is assigned to each first entity which is valid only for mail order, telephone order, or internet transactions, and which is used for multiple transactions with multiple merchants.

35. (new) A method as recited in claim 27, wherein the second entity uses the SCN to authenticate the first entity.